REMARKS

On page 2 of Paper No. 19, the Examiner, in paragraph 1, indicates that the amendment filed 24 July 2003 is objected to under 35 U.S.C. §132 because is supposedly introduces new matter by the addition of claims 18-40, and erroneously requires that such new matter be canceled in response to Paper No. 19.

The error is two fold: first, the claims do not introduce new matter; and second, the rejection of claims 18-40 under 35 U.S.C. §112, first paragraph in paragraph 3 of Paper No. 19, is an issue subject to appeal.

Accordingly, claims 18-40 do not need to be canceled until the issue under 35 U.S.C. §112, paragraph one is decided on appeal.

In paragraph 2 of Paper No. 19, the Examiner indicates that the Applicant's arguments filed 6 November 2003 were considered and deemed non-persuasive. The Applicant clearly quoted a section of the specification that provided support for claim 32, and identified where such support is found in the drawings.

Additionally, the Examiner requests that the Applicant show where support for the "amendments to the claims" and the "subject matter of the added claims" is found in the original specification, by citing page and line number.

The Applicant believes this request places an undo burden on the Applicant because the Examiner fails to identify which feature(s) of the claims he deems to be unsupported by the original specification.

We note that there has been no rejection nor objection regarding claims 1-3, 5-7 and 9-17 and

the amendments thereto. Additionally, most of the features of new claims 18-40 are found in claims 1-3, 5-7 and 9-17. Accordingly, if the features of presently presented claims 1-3, 5-7 and 9-17 have not been objected to under §132 nor rejected under §112, first paragraph, then the Applicant should not be required to identify where these same features found in claims 18-14 are found in the original specification.

That is, the Examiner (PTO) has not established a *prima facie* showing that any of the features of claims 18-40 are new matter. The burden is on the PTO to establish a *prima facie* basis of objection/rejection, and the burden to show otherwise does not shift to the Applicant until such a *prima facie* showing is established by the PTO.

In paragraph 4 of Paper No. 19, claims 18-40 have been rejected under 35 U.S.C. §112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one of ordinary skill in the art that the Applicant had possession of the claimed invention at the time the application was filed. The applicant respectfully traverses this rejection for the following reason(s).

The Examiner has not identified what subject matter, *i.e.*, which feature(s), of claims 18-40 the Examiner considers to be inadequately described in the specification in such a way as to reasonably convey to one of ordinary skill in the art that the Applicant had possession of the claimed invention at the time the application was filed.

For example, claim 18 calls for *a certificate authority for generating manufacturer key information and generating first key information for giving an authorization to supply said digital content.* Such a certificate authority (CA) for generating manufacturer key information (MK_{PD}) and

generating first key information (first authentication qualification key (public key) 11) for giving an authorization to supply said digital content is shown in Fig. 1 as element 110 (originally authorization unit 10).

Additionally, claim 18 calls for *a terminal supplier supplying a terminal, said terminal supplier outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said terminal supplier embedding the manufacturer key information in said terminal.* Such a terminal supplier 20 supplying a terminal (originally portable device 50), said terminal supplier 20 outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said terminal supplier embedding the manufacturer key information in said terminal is shown in Fig. 1 as element 120 (originally: a portable terminal supplying means 20 outputs the first registration request signal to authorization recognition unit 10 and receiving the manufacturer key and a manufacturer key data generated by authorization recognition unit 10 in accordance with the first registration request signal).

Also, claim 18 calls for *a content supplier sending a second registration request signal to the certificate authority, said certificate authority and said content supplier sharing a first secret channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said digital content from said second key information.* Such a content supplier 30 sending a second registration request signal to the certificate authority 10, said certificate authority and said

content supplier sharing a first secret (secure) channel, said content supplier receiving and storing said first key information from the certificate authority through said first secret channel for supplying said digital content, said content supplier generating and outputting second key information for giving an authorization to receive and reproduce said digital content from said second key information is shown in Fig. 1 as element 130 (originally Internet service provider 30). The present invention relates to a system for preventing an illegal copy of digital contents, and more particularly to a system for preventing an illegal copy of digital contents which forms secret channels between all the systems connected to users and exchanges contents through the formed secret channels in order to prevent digital contents from an illegal copy. Fig. 3 shows how for an ISP to register to CA and what information to get from CA. For an ISP to register to CA, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between CA and itself by EC_DH(CA, ISP).

Further, claim 18 calls for *a personal computer sending a third registration request signal to the content supplier for obtaining said second key information, said personal computer having public key information of said certificate authority, said personal computer and said content supplier sharing a second secret channel, said personal computer verifying said first key information inputted from the content supplier by using said public key information of said certificate authority and receiving the second key information through said second secret channel, said personal computer receiving said digital content through said second secret channel.* Such a personal computer is shown as element 140 (originally PC 40).

Further yet, claim 18 calls for *said terminal manufactured by said terminal supplier for reproducing said digital content and reading a storage medium, said terminal transferring the*

embedded manufacturer key information to said content supplier through said personal computer to be verified by said content supplier, said terminal and said personal computer sharing a third secret channel for transferring said digital content between said terminal and said personal computer, said terminal receiving and function-processing a physical address of a bad sector of the storage medium, a random number generated and stored in a spare area of said terminal and a secret channel key generated in said terminal to obtain a processed value, said terminal encrypting a header of the digital content with the processed value. Such a terminal is shown in Fig. 1 as element 150 (originally portable device 50).

Even further, claim 18 calls for *said storage medium transmitting said physical address of the bad sector, storing said random number as a key value generated from said terminal, storing as a sector data the encrypted header of the digital content and encrypted header information encrypted by using the result of function processing*. Such a storage medium is shown in Fig. 1 as element 160 (originally storage medium 60).

As can be seen from the above, each of the elements 10-60 of original Fig. 1 have been adequately described in the specification in such a way as to reasonably convey to one of ordinary skill in the art that the Applicant had possession of the claimed invention at the time the application was filed.

Should the Examiner have an issue with a specific feature of the claims thought to be inadequately disclosed, the Applicant will attempt to identify where such feature is originally disclosed. Otherwise, the rejection should be withdrawn.

Claims 1-3, 5-7, 9-23 and 25-40 were rejected under 35 U.S.C. §102(e) as being anticipated by Downs (6,574,609). The applicant respectfully traverses this rejection for the following reason(s).

Claim 1 calls for, in part, *a certificate authority for generating manufacturer key information and generating first key information for giving an authorization to supply said encrypted digital content*. The *manufacturer key information* is provided to *a portable terminal supplier supplying a portable terminal*. A portable terminal is, for example, an end-user device similar in many ways to the End-User Device 109 disclosed in Down's.

With respect to the claimed *certificate authority for generating manufacturer key information*, the Examiner refers us to Downs' "Clearinghouse," which is described as having the function of providing licensing authorization by enabling intermediate or End-User(s) to unlock content after verification of a successful completion of a licensing transaction.

Down's discloses, however, that license control requires that a Content Provider 101, a Electronic Digital Content Store 103, and a Clearinghouse 105 have bona-fide cryptographic digital certificates from reputable **Certificate Authorities** that are used to authenticate those components. The End-User Device 109 are not required to have digital certificates.

Accordingly, Downs clearly differentiates well known **Certificate Authorities** from Downs' Clearinghouse 105. Therefore, under §102, Downs' Clearinghouse is not equivalent to a well known **Certificate Authority**, and it is clear error to suggest that Downs' Clearinghouse corresponds to the applicant's claimed ***certificate authority***.

"There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps clinic & Research*

Foundation v. Genentech, Inc., 927 F.2d 1565, 18 USPQ2d 1001, 18 USPQ2d 1896 (Fed. Cir. 1991).

Note that in order for an anticipation rejection to be proper, the anticipating reference must disclose exactly what is claimed. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Therefore, since Downs' Clearinghouse does not correspond to the claimed *certificate authority*, the rejection is deemed to be in error for failing to disclose exactly what is claimed, and the §102 rejection of claims 1-3, 5-7, 9-16 and 18-22, each of which include the feature of a *certificate authority*, should be withdrawn.

Additionally, according to the Applicant's disclosed invention, the Manufacturer Key, MK_{PD}, which is a pre-set manufacturer key in a tamper resistant area within the PD (SDMI (Secure Digital Music Initiative) Compliant Portable Device), is to be used for the secure registration of a PD to LCM (Licensed SDMI (Secure Digital Music Initiative) Compliant Module). Prior to manufacturing PD, the manufacturers should register to the CA **(Certificate Authority)** to get their manufacturer key, MK_{PD}, and its certificate, $Cert_{CA}(ID_{MK})$, and then produce the SDMI Compliant Portable Devices by using them. Where such registered manufacturer keys are securely stored in the CA's DB (database) and only the CA maintains the information. The manufacturer should keep their manufacturer-key and its certificate safe, maintain them securely, and embed them in a tamper resistant area of the manufactured PDs during manufacture of the PDs.

According to Downs' disclosure the "End-User Device 109 are not required to have digital certificates." Additionally, Downs discloses the End-User Device(s) 169 do not need to include certificates in their SC (Secure Container) because many End-User(s) do not bother to acquire a certificate or have certificates issued by non bona-fide **Certification Authorities**. In the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 105 has the option of issuing certificates to the Electronic Digital Content Store(s) 103. This allows the End-User Device(s) 109 to independently verify that the Electronic Digital Content Store(s) 103 have been authorized by the Secure Digital Content Electronic Distribution System 100.

In Downs' system the "architecture requires that the Electronic Digital Content Store(s) 103 assigns a unique application ID to the downloaded Player Application 195 and that the End-User Device(s) 109 stores it for later application license verification." And that Downs' license control "requires that the Content Provider(s) 101, the Electronic Digital Content Store(s) 103, and the Clearinghouse(s) 105 have bona-fide cryptographic digital certificates from reputable Certificate Authorities that are used to authenticate those components. The End-User Device(s) 109 are not required to have digital certificates."

Accordingly, the *portable terminal* in Downs (End-User Device 109) does not receive and store in a tamper resistant area, *manufacturer key information* provided by a *certificate authority* as required by the instant claims, but instead stores a **unique application ID** to a downloaded Player Application 195, the unique application ID being **assigned by an Electronic Digital Content Store 103** (not a Certificate Authority nor a Clearinghouse).

Therefore, Downs fails to exactly what is claimed, thus the §102 rejection of claims 1-3, 5-7, 9-16, 18-23 and 25-40, each of which include the feature of a *manufacturer key* or *manufacturer key*

information, should be withdrawn. is not proper and should be withdrawn.

Claim 1 also calls for *a portable terminal supplier supplying a portable terminal, said portable terminal supplier outputting a first registration request signal to said certificate authority and receiving the manufacturer key information generated by said certificate authority in accordance with the first registration request signal, said portable terminal supplier imbedding the manufacturer key information in said portable terminal.*

The Examiner fails to identify where Downs discloses such a *portable terminal supplier supplying a portable terminal.* Note, *Ex parte Levy*, 17 USPQ2d 1461, 1462 (1990) states:

> "it is incumbent upon the examiner to identify wherein each and every facet of the claimed invention is disclosed in the applied reference."

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly what is claimed. Accordingly, the §102 rejection of claims 1-3, and 18-22, each of which contains the feature of a *terminal supplier*, is not proper and should be withdrawn.

The foregoing arguments have shown that each of claims 1-3, 5-7, 9-6, 18-23 and 25-40 are not anticipated by Downs. Additionally, claim 17 is not anticipated by Downs because Downs fails to disclose *a terminal receiving a physical address of a bad sector of a storage medium.* The Examiner fails to identify where Downs discloses such *a terminal receiving a physical address of a bad sector of a storage medium.* Note, *Ex parte Levy*, supra.

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly

what is claimed. Accordingly, the §102 rejection of claim 17 is not proper and should be withdrawn.

Claim 24 was rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Downs in view of Davis (6,041,314). The Applicant respectfully traverses this rejection for the following reason(s).

Claim 24 depends from claim 23. Claim 23 calls for *a second cryptosystem encrypting and ~~transfering~~ transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider, said server establishing a third secure channel to said terminal after the validation of the manufacturer key information.*

As noted above with respect to the §102 rejection, Downs fails to disclose *manufacturer key information.*

Accordingly, since Downs fails to disclose such *manufacturer key information* the cannot possibly be a second cryptosystem encrypting and transferring manufacturer key information embedded in a terminal from the terminal to a content provider to be verified by the content provider, such that the server will establish a secure channel to the terminal after the validation of the manufacturer key information disclosed in Downs. Examiner fails to identify where Downs discloses *transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider.* Note, *Ex parte Levy*, supra.

Davis was not applied as a teaching of *manufacturer key information* nor as a teaching of

transferring manufacturer key information embedded in a terminal linked to said server from said terminal to said content provider to be verified by said content provider.

Therefore, the Examiner fails to provide *prima facie* evidence that Downs discloses exactly what is claimed. Accordingly, the §102 rejection of claim 23 is not proper and, since claim 24 depends from claim 23, the §103 rejection is not proper and should be withdrawn.

The examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

A fee of $110.00 is incurred by filing of a petition for one month extension of time. Applicant's check drawn to the order of the Commissioner accompanies this Amendment. Should the check become lost or detached from the file, the Commissioner is authorized to charge Deposit Account No. 02-4943 and advise the undersigned attorney accordingly. Also, should the enclosed check be deemed to be deficient or excessive in payment, the Commissioner is authorized to charge or credit our deposit account and notify the undersigned attorney of any such transaction.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P55690
Date: 4/23/04
I.D.: REB/MDP